

UNITED STATES DISTRICT COURT  
DISTRICT OF MASSACHUSETTS

---

ARBOR NETWORKS, INC.,

Plaintiff,

v.

WILLIAM E. RONCA III, RICHARD SHIRLEY,  
DOUGLAS FLEMING, JAMES GILL, JAMES  
NEEL, JASON MCEACHIN, MICHAEL L.  
PORTER, ANDREW HENKART, PAUL  
SCANLON, MICHAEL HOLLYMAN, and  
RED LAMBDA, INC.,

Defendants.

---

C.A. No. 12-11322

**PLAINTIFF’S OPPOSITION TO DEFENDANTS’ MOTION TO CLARIFY  
OR MODIFY PRELIMINARY INJUNCTION**

Plaintiff Arbor Networks, Inc. (“Arbor” or “Plaintiff”) hereby opposes Defendants’ Motion to Clarify or Modify Preliminary Injunction (“Motion to Clarify”). As grounds therefore, and as set forth more fully below, Arbor states that the Order imposes no conflicting duties on the Defendants, and that the Defendants’ concerns, while entirely unfounded, may nonetheless be addressed by the Defendants’ prompt creation of forensic images of the systems and media that may contain Arbor’s trade secrets or other confidential business/financial information.

**1. The Order Does Not Impose Conflicting Obligations On Defendants**

With respect to Defendants’ claim that the Order potentially imposes conflicting obligations, Arbor states that Sections 2 and 3 of the Order are quite clear in the imposition of an absolute duty on the part of Defendants to preserve (*i.e.*, to not destroy, alter, delete, or otherwise

spoliate) any data that may be relevant to this lawsuit, including any data belonging to Arbor or concerning the circumstances of the Individual Defendants' departure from Arbor. By contrast, Section 1 of the Order is intended to foreclose the Defendants' use, disclosure, or retention—other than as necessary to comply with Defendants' absolute duty to preserve—of Arbor's trade secrets or confidential business/financial information. Section 1's prohibition on the retention of confidential Arbor information is properly understood as imposing an obligation on Defendants to return or delete Arbor information at the conclusion of this action (or sooner pursuant to party agreement), with any such deletion performed not by the Defendants themselves, but instead by a forensic expert in accordance with an agreed-upon protocol between the parties.

It is bedrock black-letter law that to the extent the Defendants are currently in possession, custody, or control of potentially relevant information as described by Section 1 of the Order, Defendants unambiguously have a duty to forensically preserve that information until such time as the parties can reach agreement on a remediation plan, and that creation of forensic images (or "mirror images") is the best way (and indeed, the only adequate way) to preserve such data. In *United Factory Furniture Corp. v. Alterwitz*, 2012 U.S. Dist. LEXIS 48795 (D. Nev. April 6, 2012), the court stated that "the defendants are under a duty to preserve relevant evidence, including electronically stored information. Considering the circumstances of this case, the court finds mirror-imaging is appropriate to maintain the status quo." *Id.*, \*10. The court went on to note that the allegations in the complaint related to the defendants' unlawful access to and destruction, copying, and altering of information stored on plaintiff's computers, and thus that "[i]nformation stored on the defendants' computers or electronic devices is directly relevant to this action. Fed. R. Civ. P. 26(b)(1). For the action to be fairly litigated, defendants' computers must remain unaltered." *Id.*, \*11-12. The court went on to hold that the evidence sought to be

preserved through mirror-imaging “could not be obtained through simple document production, as information describing the history, tracking, or management of an electronic file is usually not apparent via a hard copy or a screen image.” *Id.*, \* 13. So too must portions of Defendants’ computer systems be preserved through forensic imaging, in light of the evidence already obtained by Plaintiff that defendants Gill and McEachin permanently deleted data on their Arbor-issued computers, as well as this Court’s Order requiring Gill, McEachin, and Red Lambda to preserve relevant data. *See also Capitol Records, Inc. v. Alaujan*, 2009 WL 1292977, \*1 (D. Mass. May 6, 2009) (in authorizing mirror imaging of relevant computers, this Court determined that “where the computer itself is at the heart of the litigation . . . it is plainly relevant under Fed. R. Civ. P. 26(b).”); *Balboa Threadworks, Inc. v. Stucky*, 2006 WL 763668, \*3 (D. Kan. March 24, 2006) (“It is not unusual for a court to enter an order requiring the mirror imaging of the hard drives of any computers that contain documents responsive to an opposing party’s request for production of documents. Thus, in similar cases where trade secrets and electronic evidence are both involved, the Courts have granted permission to obtain mirror images of the computer equipment which may contain electronic data related to the alleged violation. This is one method of assuring the preservation of evidence since electronic evidence can easily be erased and manipulated, either intentionally or unintentionally (by overwriting through continued use of the computer).”) (citations omitted).<sup>1</sup>

Likewise, in *Ferron v. Search Cactus, L.L.C.*, 2008 WL 1902499 (S.D. Ohio April 28, 2008), where defendants requested an inspection of plaintiff’s computer systems, the court noted that continued operation of computers results in the routine alteration and deletion of information of potentially discoverable information. Accordingly, where the plaintiff had failed to properly

---

<sup>1</sup> Arbor contends that by virtue of this Court’s Preliminary Injunction Order, the Court has already implicitly required mirror imaging so as to preserve relevant data. However, to the extent such a requirement was not made explicit, Arbor respectfully requests that this Court so order.

preserve information, the court determined that the defendants should be permitted to access the plaintiff's computer systems. This determination was based on the fact that the plaintiff's computers "contain[ed] the only available documentary evidence" of the claims at the heart of the action (as is the case here). *Id.* at \*2. Plaintiff claimed that he had saved and preserved all of his commercial email, that the defendants never requested a litigation hold, and defendants never provided notice of their intent to inspect computers prior to service of formal discovery requests. The court found these points unavailing, noting that "[e]ven in Plaintiff has preserved and saved his 'commercial email,' those actions do not sufficiently fulfill his duty to preserve evidence, which 'arises when the party has notice that the evidence is relevant to litigation or when a party should have known that the evidence may be relevant to future litigation.'" *Id.* at \*3 (citing *Zubulake v. UBS Warburg LLC*, 220 F.R.D. 212, 216 (S.D.N.Y. 2003). Further, the court noted, "Plaintiff's duty to preserve this information is independent of whether Defendants requested a litigation hold." *Id.* Later, the court noted that the plaintiff himself had "caused this issue to become problematic because of his failure to place a sufficient litigation hold on his computer systems as of the date he anticipated this litigation." *Id.* at \*4.<sup>2</sup>

Similarly, even in the absence of a court order, the Defendants in this action should have taken appropriate steps to preserve all potentially relevant data, including electronically-stored information, when they first received notice that such evidence might be relevant to future litigation. Indeed, to the extent the Defendants have (inexplicably) failed to preserve relevant data upon notice of potential litigation, this Court's Order dated August 8, 2012 makes crystal clear the Defendants' obligation to preserve via forensic imaging those computer systems that

---

<sup>2</sup> In light of the fact that the only available documentary evidence related to certain claims at issue in the action resided on the plaintiff's computer systems, the court ordered the plaintiff's forensic computer expert to create a mirror image plaintiff's computer systems, and ordered that the plaintiff store the images safely. The court then crafted a protocol by which privileged or irrelevant materials would be deleted by a forensic expert, and the remaining materials would be produced to defendants.

may contain potentially relevant information. Thus, as stated above, in order to comply with the duty to forensically preserve potentially relevant information, Defendants must create and maintain forensic images of the systems and media that may contain Arbor's trade secrets or confidential business/financial information, including but not limited to bit-for-bit forensic images of the Individual Defendants' workstations and removable media, complete snapshots of the Individual Defendant's corporate email accounts, and forensic copies of any network shares or other locations accessible by and/or associated with the Individual Defendants. Defendants should then abide by their concomitant obligation not to disclose or make any use of Arbor's confidential information or trade secrets, other than as may be required in connection with discovery in this action.

While Arbor vehemently disagrees with Defendants' assertion that the Order is somehow inconsistent and that any amendments thereto are required, should this Court deem some additional clarification necessary, Arbor suggests that Section 1 be modified by inserting the explanatory parenthetical, "(other than as set forth in Sections 2 and 3 below)," immediately following the word "retaining" to make clear that Defendants' duties to preserve take precedence over the proscriptions set forth in Section 1 of the Order. This addition, in conjunction with the Defendants' discharging their obligation to create and maintain forensic images as set forth above, would readily address any of the Defendants' concerns related to potential spoliation.

## **2. Defendants' Concerns Regarding Alleged "Impossibility Of Performance" Would Be Resolved By Creating Forensic Images**

Defendants should not be heard to complain about the burdens associated with complying with their fundamental duties to preserve in this action. By promptly taking the aforementioned steps to create forensic physical images of the pertinent systems and media containing information covered by the terms of the Order, a pristine copy of those files can then be set aside

to assure compliance with the Order and avoid the risk of those files being altered or deleted (whether intentionally or inadvertently) in violation of the Order.

Defendants' concerns regarding the return of property to Arbor are likewise unfounded. Once the requisite forensic images have been created, the parties can work together to reach an agreement on a remediation protocol through which reports would first be generated of the contents of the drives and media that were imaged, with any Arbor data flagged for permanent deletion on the original devices (such deletion to be performed by a forensic expert), followed ultimately by the destruction of the images themselves.

Defendants' exhortations regarding the difficulties associated with preserving cloud-based data are nothing but a red herring, as techniques are readily available to ensure the adequate preservation, and eventual remediation, of information that resides on the cloud. Defendants should work with a forensic expert to ensure that all relevant data is preserved, including data that may reside in the cloud. Defendants should not take any steps that may result in the impermissible alteration of metadata, such as moving data from one storage medium to another, without first engaging the services of a forensic examiner to perform the requisite collections and/or consulting with Arbor's counsel and receiving express permission to so remove data.

### **CONCLUSION**

For the reasons set forth above, this Court should deny Defendants' Motion to Clarify or Modify Preliminary Injunction in its entirety. In the alternative, should this Court decide to amend the Order, Arbor respectfully requests that this Court add the parenthetical, "(other than as set forth in Sections 2 and 3 below)," immediately following the word "retaining" in Section 1 of the Order.

Respectfully submitted,

ARBOR NETWORKS, INC.

By its attorneys,

/s/ Dawn Mertineit

Katherine E. Perrelli (BBO #549820)

Dawn Mertineit (BBO #669988)

SEYFARTH SHAW LLP

World Trade Center East

Two Seaport Lane, Suite 300

Boston, Massachusetts 02210

(617) 946-4800

Dated: August 14, 2012

**CERTIFICATE OF SERVICE**

I hereby certify that this document filed through the ECF system will be sent electronically to the registered participants, as identified on the Notice of Electronic File (“NEF”), and paper copies will be sent to those indicated as non-registered participants on August 14, 2012, by first class mail.

/s/ Dawn Mertineit

Dawn Mertineit